System Certification & Accreditation

Introduction
Information Services (IS) and/or the IR system owner/administrator share the responsibility of ensuring that IR systems and processes are setup, established and maintained in a manner consistent with existing information system security legislation, institutional standard practices and business best practices. These standards and practices include, but are not limited to: the protection of information and information resources (IR); limitation/restriction of access and use of information and IR to a standard of “Appropriate Use”; and ongoing monitoring and re-evaluation of IR system to ensure continued applicability and compliance throughout the life cycle of the system.

Purpose
This practice standard details the processes by which an information resource (servers, workstations, printers, etc.) is registered (identified and associated with a data owner), certified (verification that IR security measures are in place and producing the desired results) and accredited (acceptance of risk and applicableness in scope for network operations).

Audience
The UTMB System Certification & Accreditation Practice Standards apply equally to all individuals with responsibility for installing, maintaining or administrating information resources. These practice standards also apply to data owners and those tasked with IR security functions.

Implications
- All information resources must meet a minimum pre-defined set of security criteria as described in the IS Practice Standards.
- Data owners (or designate) must be cognizant of data sensitivity, measures in place to meet security criteria and the effectiveness of those measures.
- The ISO is the final authority with regards to accreditation of information resources. Accreditation (or a decision not to accredit) will be based on the totality of the certification information provided and the recommendation of the NSS and the Office of Information Security.
- IS will disable the network (or full system) operations of any IR which does not meet or maintain accreditation standards.
<table>
<thead>
<tr>
<th>Practice Standards</th>
</tr>
</thead>
<tbody>
<tr>
<td>- Data owners, information resource installers/administrators, and those tasked with IR security functions will periodically or when planning, purchasing, installing or upgrading IR, review the applicable practice standards located online at: <a href="http://www.utmb.edu/infosec/PoliciesStandards/Index.asp">http://www.utmb.edu/infosec/PoliciesStandards/Index.asp</a></td>
</tr>
<tr>
<td>- The data owner or administrator will conduct a risk assessment on any newly implemented system or any existing systems that has had significant changes to its configuration.</td>
</tr>
<tr>
<td>- An interim “authorization to operate” will be provided once the “System Registration &amp; Certification Request Form” has been completed.</td>
</tr>
<tr>
<td>- Data owners or administrators will provide verification and/or assurance that administrative controls required by the practice standards, such as regular, scheduled backups are in place and operational.</td>
</tr>
<tr>
<td>- IS will perform scans, tests and other procedures to verify the existence and performance of technical controls required by the practice standards, such as anti-virus configuration.</td>
</tr>
<tr>
<td>- The data owner or administrator will institute or develop compensating controls for all security controls which, for technical or business reasons, cannot be implemented as required by the practice standards.</td>
</tr>
<tr>
<td>- In the absence of required or compensating controls, the data owner will request, in writing, a waiver from the security control. (NOTE: the waiver request must include a justification and a “Risk Assumption” document under signature of the data owner AND the UTMB Information Security Officer.)</td>
</tr>
<tr>
<td>- The Office of Information Security will make accreditation recommendations to the IRM as requested.</td>
</tr>
<tr>
<td>- The data or the assigned Information Security Administrator will provide all certification documentation and findings to the Information Security Officer for final accreditation determination</td>
</tr>
</tbody>
</table>
System Certification & Accreditation, Continued

Practice Standards (con’t)

- If the IR is accredited, NSS will begin monitoring and quarterly scans to verify continued compliance with security controls.
- If the IR is accredited, the data owner, working with the Office of Information Security will periodically review the administrative and technical controls using the established risk assessment process to verify continued compliance with published practice standards.
- If the accreditation is declined, the ISO, at his discretion, may: allow the IR to remain in operation (interim authorization to operate) pending update certification information or accreditation recommendations; require the IR to operate in an isolated or in a stand alone mode; or require the IR to be shutdown or discontinued until IR security controls can be instituted and verified.
- The data owner or administrator will notify ISO of any significant operational or programmatic changes and will request that a new risk assessment be completed.

Disciplinary Actions

Operation of an Information Resource in violation of this policy may result in disciplinary action which may include termination for employees; a termination of employment relations in the case of contractors or consultants; or suspension or expulsion in the case of a student. Additionally, individuals are subject to loss of UTMB IR access privileges, civil and/or criminal prosecution. Additionally, the IR may be subject to disconnection, isolation and or confiscation.

References

- UTMB Acceptable Use of Information Resources Policy
- UTMB Information Resources Security Policy
- UTMB IR Security Management Practice Standards Approval Process
- UTMB IR Security Glossary
- UTMB IR Network Configuration Practice Standard
- UTMB IR Password Management Practice Standard
- UTMB IR Account Management Practice Standard
- UTMB IR Network Access Practice Standard
- UTMB IS Hardware Standards
### Definitions

(These definitions will be incorporated within the glossary)

**System Certification:** a comprehensive assessment of the management, operation and technical security controls in an information system to determine the extent to which the controls are implemented correctly, operating as intended and producing the desired outcome with respect to meeting the security requirements for the system.

**System Accreditation:** the official decision to authorize operation of an information system and to explicitly accept the risk to information, information resources and information users based on the implementation of an agreed-upon set of security controls.

**Risk Assessment/Analysis:**

**Security Controls:**

**User Authentication:** a method by which the user of a wireless system can be verified as a legitimate user independent of the computer or operating system being used.

**Virtual LAN:** a network of computers that behave as if they are connected to the same wire even though they may actually be physically located on different segments of a LAN.

**Virtual Private Network (VPN):** a network that is constructed by using public wires to connect nodes. These systems use encryption and other security mechanisms to ensure that only authorized users can access the network and that the data cannot be intercepted.

**Wired Equivalent Privacy (WEP):** an optional function that offers transmission privacy similar to a wired network.

**Wireless:** technology that permits the transfer of information between separated points without physical wire connection.

**Wireless Devices:** cellular telephone, personal digital assistants, interactive TV, wireless/IR copiers and faxes, and transport infrastructure components such as, but not limited to, transmitters, receivers, amplifiers, and antennas.

**Wireless Network:** one in which a mobile user can connect to a local area network through a wireless (radio) connection.